



2131
#5
KWS
4-30-02

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Wenbo Mao) Re: Information Disclosure
Serial No.: 09/913,003) Statement
Filed: August 8, 2001) Group: not yet assigned
For: "VERIFICATION OF THE PRIVATE) Examiner: not yet assigned
COMPONENTS OF A PUBLIC-KEY) Our Ref: B-4253PCT 618967-4
CRYPTOGRAPHIC SYSTEM) Date: October 25, 2001

RECEIVED

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

JAN 18 2002

Sir:

Technology Center 2100

In accordance with the Applicant's duty to disclose information which may be material to the examination of this application, the undersigned respectfully requests that the Examiner consider on the merits the documents listed on the enclosed Form PTO-1449 (modified) before issuing the first Office Action on the merits. We are enclosing herewith a copy of each document listed on the enclosed Form PTO-1449 (modified).

A copy of an International Search Report is enclosed herewith. The documents listed on Form-1449 (modified) include those cited in the International Search Report of International Patent Application No. PCT/GB00/00370 (3 pages).

A copy of a British Search Report is enclosed herewith. The documents listed on Form-1449 (modified) include those cited in the Search Report of British Patent Application No. GB 9902687.4 (1 page).

The filing of this Information Disclosure Statement (IDS) shall not be construed as a representation that a search has been made (37 C.F.R. 1.97(g)), an admission that the information cited is, or is considered to be, material to patentability, or that no other material information exists.

The Applicant believes that this IDS is being submitted before the issuance of a first Office Action on the merits and before the issuance of a Final Rejection or Notice of Allowance. Therefore,

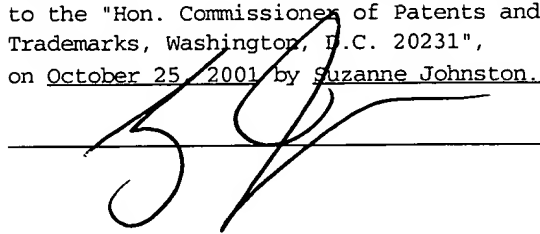
Information Disclosure Statement
USSN 09/913,003
October 25, 2001
Page 2

no official fees should be due; and this IDS should be considered on the merits. If this IDS is being submitted after the issuance of the first Office Action on the merits and before the issuance of a Final Rejection or Notice of Allowance, then the Commissioner is authorized to charge Deposit Account No. 12-0415 \$180.00 (or any other required amount), which is the fee set forth in 37 C.F.R. § 1.97(c); and this IDS should be fully considered on the merits, in accordance with 37 C.F.R. § 1.97(d). If this IDS is being submitted after the issuance of a Final Rejection or Notice of Allowance, then the Commissioner is not authorized to charge \$180.00 to Deposit Account No. 12-0415.

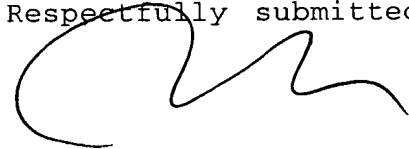
The filing of this Information Disclosure Statement shall not be construed as an admission against interest in any manner. (Notice of January 9, 1992, 1135 O.G. 13-25, at 25.)

The person making this statement is the practitioner who signs below on the basis of information supplied by an individual associated with the filing and prosecution of this application (37 C.F.R. § 1.56(c)) and on the basis of information in the practitioner's file.

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first-class mail in an envelope addressed to the "Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231", on October 25, 2001 by Suzanne Johnston.



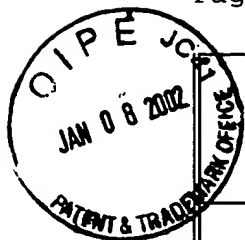
Respectfully submitted,



Richard P. Berg
Attorney for Applicant
Reg. No. 28,145

LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
(323) 934-2300

Enclosures: Form PTO-1449 (modified) (2 pages)
A copy of International Search Report of PCT/GB00/00370
(3 pages)
A copy of British Search Report of GB9902687.4
(1 page)
Copy of documents listed on Form PTO-1449 (modified)



	✓	Damgard, Ivan Bjerre, "Practical and Provable Secure Release of a Secret and Exchange of Signatures," <i>Advances in Cryptology-Proceedings of EUROCRYPT 93, Lecture Notes in Computer Science</i> , Springer-Verlag, 765, pp. 200-217 (1994).
	✓	Karanakis, E., <i>Primality and Cryptography</i> , Wiley-Teubner Series in Computer Science, John Wiley & Sons, p. 28 (1986).
	✓	Blackburn, S.R. and Galbraith, Steven D., "Certification of Secure RSA Keys," <i>Technical Report CORR 90-44</i> , University of Waterloo Centre for Applied Cryptographic Research, pp. 1-10 (May 6, 1999).
	✓	Boyar, Joan, et al., "Practical Zero-Knowledge Proofs: Giving Hints and Using Deficiencies," <i>Advances in Cryptology-Proceedings of EUROCRYPT 89, Lecture Notes in Computer Science</i> , Springer-Verlag, 434, pp. 155-172 (1990).
	✓	Galil, Zvi, et al., "A Private Interactive Test of a Boolean Predicate and Minimum-Knowledge Public-Key Cryptosystems," <i>26th FOCS</i> , pp. 360-371 (1985).
	✓	Gennaro, Rosario, et al., "An Efficient Non-Interactive Statistical Zero-Knowledge Proof System for Quasi-Safe Prime Products," <i>5th ACM Conference on Computer and Communications Security</i> , pp. 1-13 (October 1998).
	✓	Van de Graaf, Jeroen and Peralta, Rene, "A Simple and Secure Way to Show the Validity of Your Public Key," <i>Advances in Cryptology-Proceedings of CRYPTO 87, Lecture Notes in Computer Science</i> , Springer-Verlag, 293, pp. 128-134 (1988).
	✓	ISO/IEC 9798-3, "Information technology - Security techniques - Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm," International Organization for Standardization, Geneva, Switzerland, pp. 1-9 (1993).
	✓	Micali, Silvio, "Fair Public-Key Cryptosystems," <i>Advances in Cryptology-Proceedings of CRYPTO 92, Lecture Notes in Computer Science</i> , Springer-Verlag, 740, pp. 113-138 (1993).
	✓	Solovay, R. and Strassen, V., "A Fast Monte-Carlo Test for Primality," <i>SIAM Journal of Computing</i> , Vol. 6, No. 1, pp. 84-85 (March 1977).

EXAMINER	DATE CONSIDERED

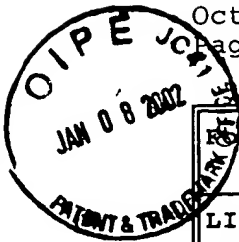
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

RECEIVED

JAN 18 2002

Technology Center 2100

Information Disclosure Statement
 USSN 09/913,003
 October 25, 2001
 Page 3



Form PTO-1449 (Modified)	ATTY DOCKET NO. B-4253PCT 618967-4	U.S. SERIAL NO. 09/913,003
LIST OF PATENTS AND PUBLICATIONS STATEMENT	APPLICANT Wenbo Mao	
	FILING DATE August 8, 2001	GROUP not yet assigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	ISSUE DATE	NAME	CLASS	SUB-CLASS	FILING DATE or 102(e) DATE IF APPROPRIATE
	4,633,036	12/86	Hellman, et al.	178	22.11	
	4,405,829	09/83	Rivest, et al.	178	22.1	

FOREIGN PATENT DOCUMENTS

DOCUMENT NUMBER	PUBLICATION DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES/NO
0 534 420 A2	3/31/93	EP			
0 202 768 A2	11/26/86	EP			

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

✓	Berger, Richard, et al., "A Framework for the Study of Cryptographic Protocols," <i>Advances in Cryptology-Proceedings of CRYPTO 85, Lecture Notes in Computer Science</i> , Springer-Verlag, pp. 87-103 (August 1985).
✓	Blum, Manuel, "Coin flipping by telephone: a protocol for solving impossible problems," <i>Proceedings of 24th IEEE Computer Conference (CompCon)</i> , pp. 133-137 (February 1982).
✓	Goldwasser, Shafi, "Multi-Party Computations: Past and Present," <i>Proceeding of the 16th Annual ACM Symposium on Principles of Distributed Computing</i> , pp. 1-6 (August 1997).
✓	Camenisch, Jan and Michels, Markus, "Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes," <i>Advances in Cryptology-EUROCRYPT 99, Lecture Notes in Computer Science</i> , Springer-Verlag, 1592, pp. 106-121 (1999).
✓	Liskov, Moses and Silverman, Robert D., "A Statistical Limited-Knowledge Proof for Secure RSA Keys," <i>5th ACM Conference on Computer and Communications Security</i> , IEEE P1363 Research Contributions, pp. 1-14 (1998).